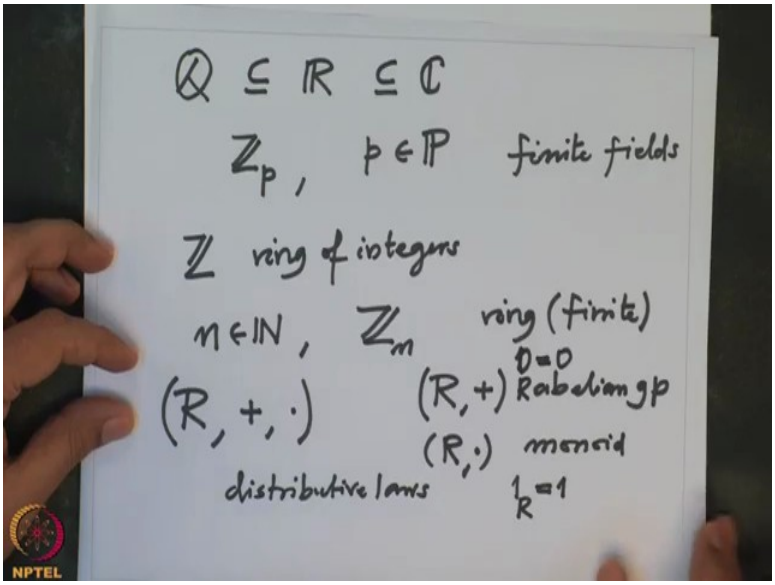
Galois Theory
Professor Dilip P. Patil
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 03 – Polynomials and Basic properties

In the last lecture we saw some examples of fields. In today's lecture we will see more examples of fields. And more generally we will see some examples of rings also. Recall that last time, last lecture we saw the field of rational numbers, field of real numbers, field of complex numbers. So $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. In addition to this standard number systems that we study in schools and colleges, in addition to that we have seen these module operations, $\mathbb{Z}$ mod p, where p varies in the set of prime numbers.

(Refer Slide Time: 1:40)



So this is a family of finite fields. This is also called finite fields. These are finite sets and on that there are this congruent mod p is a binary operation. More generally I will should you there are other examples of finite fields as well. But before I do all these things, I need more general examples of rings. The only examples of rings we know now so far are apart from these fields, the ring of integers, is ring of integers.

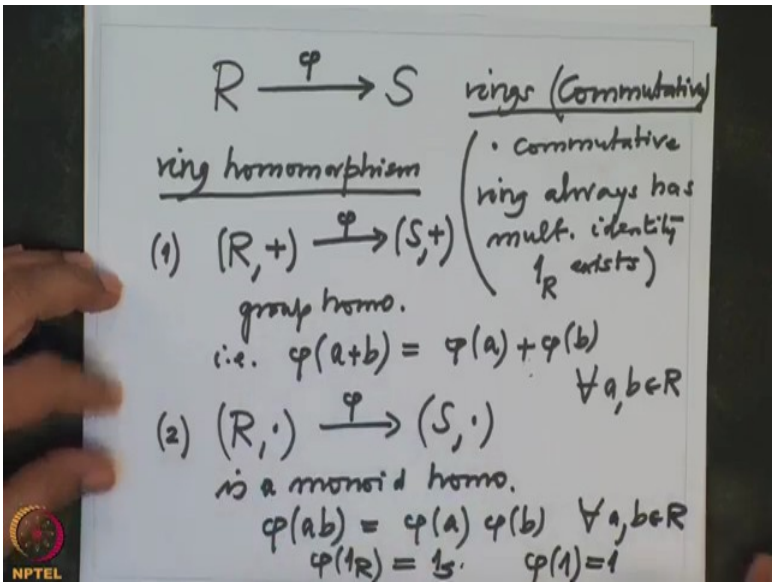
And I want to construct more examples from the given examples. That will always be our strategy to construct more examples from the given examples. So this process will be natural. So if I take instead of p, any n, natural number, lasting also this $\mathbb{Z}_n$, this is also ring, it is a finite

ring. So in general when one says ring, R is a ring, that means R is a set and it had two binary operation, addition and multiplication.

And these multiplication and additions are connected by distributive laws. And obviously R with the addition like in the case of field, this is a Abelian group and R with multiplication this is only a monoid. So I remind you monoid means a set with the binary operation which is associative and it has a neutral element. And that neutral element is usually denoted by 1_R or simply 1, means there is no confusion.

And additive identity is denoted by 0_R which is also denoted by 0 when there is no confusion. So this is a ring and when we have two rings, then usually one compares them like a set, like we were comparing the sets by maps. So these maps should not be just arbitrary maps but they should be compatible with the ring structure. Ring structure means these two binary operations, plus and multiplication.

(Refer Slide Time: 4:33)



So when I have two rings, R and S, before I go on more generally, when I said rings, even earlier I always mean commutative. That means anyway the addition operation is commutative but in addition to that the multiplication operation is also commutative. And we will assume always that ring has always multiplicative identity. Ring always has multiplicative identity, multiplicative neutral element. That means 1 always exists, 1_R exist always in our definition. This is standard assumption. I will not keep saying again and again.

All rings we will consider in this course will be commutative rings with unity. That means multiplicative identity. When it is not the case I will specify it explicitly. So when we have two rings, R and S, so remember that these have addition and multiplication. But we are not going to make distinction between the notation because otherwise it might become more and more complicated to write it.

So a map ϕ between the set R to S is called a ring homomorphism. Actually what I am doing right now is a part of my prerequisite, I want to assume in this course. But for the sake of completeness I want to recall some basic definitions. This means as Abelian group, so (R,+) is called additive group of R. And (S,+) plus is called additive group of S.

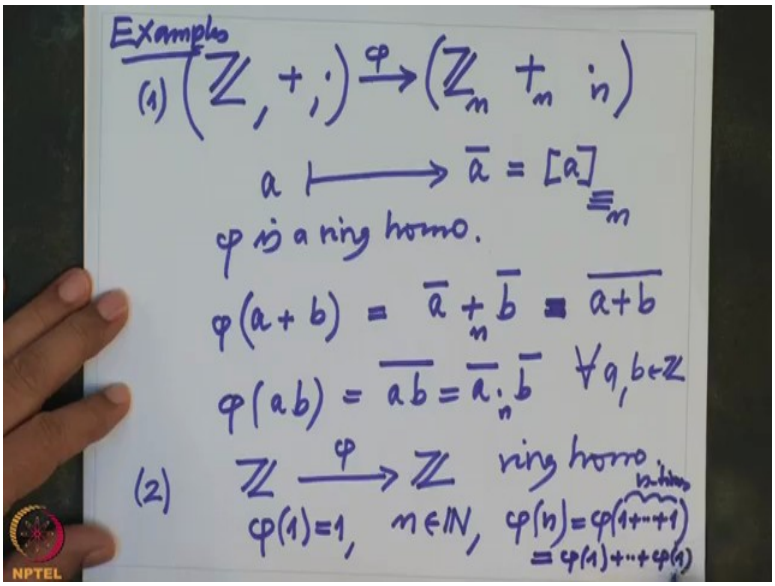
If I think of this phi as a map from this Abelian group to this Abelian group, it should be a group homomorphism. That simply means that this phi restricts the addition. $\phi(a+b)=\phi(a)+\phi(b)$, for all $a,b\in R$. So remember while writing one should be clear that when you write this plus, that means you are adding in R with respect to + in R. And when you are taking images and adding them, you are adding in S.

So that means this plus, though they look the same symbols, this is in R and this is in S. So this is clear from the writing. We cannot be going specifically, this is in R and this is in S, otherwise we will not lead to much material in this course. So second one is, it also respect the multiplication. So (R,.) to (S,.), the same field, is a monoid homomorphism. Monoid homomorphism means it respect the multiplication.

So ϕ, now multiplication, $\phi(a).\phi(b)=\phi(ab)$, for all a, b in R. And again I do not, only just now the last time I will say that this multiplication is in R. This multiplication of the images is in S. In addition to this, usually it is assumed that $\phi(1_R)=1_S$. 1_R means a multiplicative identity in R and 1_S means multiplicative identity in S.

This also I will drop eventually. I will just simply write $\phi(1)=1$. Usually in many books this is not assumed but we are assuming this. So a map between R to S satisfying both these properties is called a ring homomorphism.

(Refer Slide Time: 9:53)



For example, so any concept we should be supporting by examples. For example, let us take our ring $\mathbb{Z}$. And we have this ring $\mathbb{Z}_n$, this is modulo operation here. This plus, dot, you remember and this is decent. This again we should suppress it but only for today let me just do it. So the map here is, just take any a in $\mathbb{Z}$ and map it to a bar, a bar means equivalence class of a under this binary operation congruent modulo n.

So we check that, one should check that. So these are examples. One checks that this map ϕ is a ring homomorphism. So that means what do I have to check? I have to check that if I take two integers a and b and add them usually and take the image under this ϕ, this is $\bar{a}+\bar{b}$. But remember $\bar{a}+\bar{b}$ is defined as usually add that a + b and take the remainder of that a + b. So these two operations are same. That is what we have to check. That I will leave it for you to check. This is for every a and b integers.

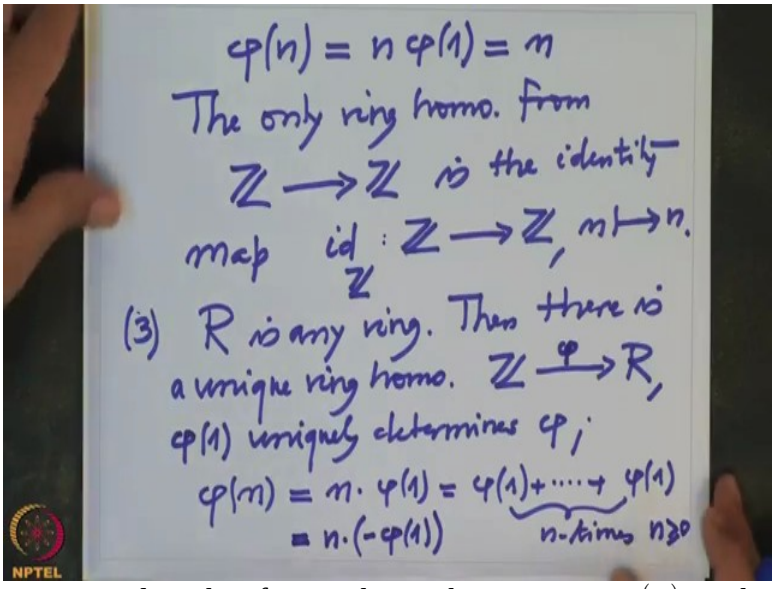
So that will mean that this phi restrict the, respect the addition, plus. So strictly speaking I should write suffix n here. But I will not do so. And also this map usually, I will come back to more of this type. Similarly we will have to check that $\phi(a.b)=\overline{ab}=\bar{a}\bar{b}$. And this dot is actually mod n. So this is a very natural example of a ring homomorphism. And this is not so special. Soon I will give you more examples of this kind.

But second thing I will leave it for you to check. Every ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ let us say, $\mathbb{Z}$ to $\mathbb{Z}$. If I have a ring homomorphism, then what can it be? Let us try to analyze. So first of all, note that by our definition 1 has to go to 1. So $\phi(1)=1$. Moreover, if I

take any integer n, if n is positive in the natural number, then phi n which is

$= 1+1+\ldots n\,time$

(Refer Slide Time: 13:26)



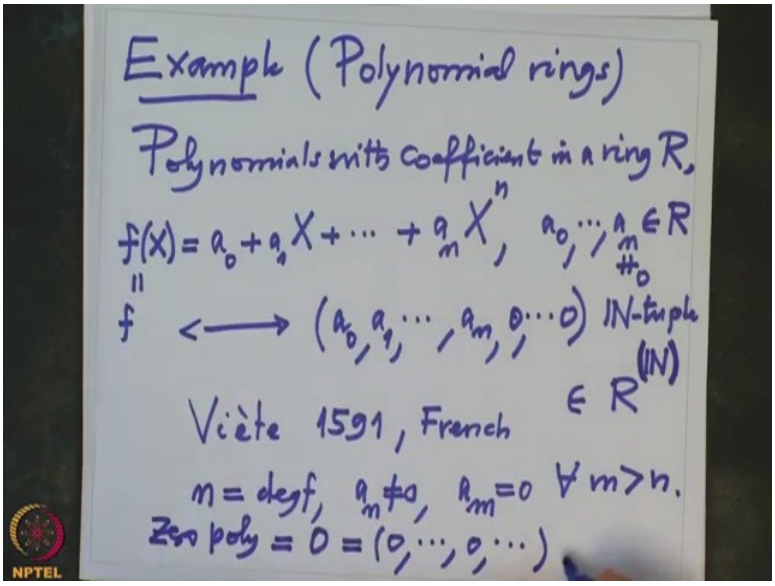
So that means what we noted is phi of any n has to be n times $\phi(1)$. That means this phi is uniquely determined by the image of 1, which is 1 only in this. So this is n. So that means we check that the only ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is identity map. So the only ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is the identity map which is denoted by $id_{\mathbb{Z}}$. This is a map $\mathbb{Z}$ to $\mathbb{Z}$, n goes to n. So that is only. In fact, why this?

In fact, more generally, if R is any ring, then there is a unique ring homomorphism from $\mathbb{Z}$ to R. And it will be, obviously it is determined by, if you call it ϕ , that is uniquely determined by $\phi(1)$. $\phi(1)$ of 1 determines ϕ . In fact, if I take any n, $\phi(n)$ will be equal to n times $\phi(1)$. Remember n times ϕ (1) means $\phi(1)+\phi(1)+\phi(1)+\ldots$, added n times.

When I say, when n were negative, then one should use the additive inverses of this one. So this is when n is bigger equal to 0, and when n is negative, then it is in fact n of $-\phi(1)$. Remember $-\phi(1)$ makes sense in the ring because it is the additive inverse of $\phi(1)$. So this is very important map, I will soon use it. I will soon use this to define something about the field. Anyway, so we have ring homomorphism.

So ring (homomorph), in every subject like if you are studying group study, then you use group homomorphism to compare two groups. If you are studying ring theory, you use ring homomorphism to compare rings. If you are studying field theory, then you use homomorphism of fields. Homomorphism of fields are nothing but homomorphism of the rings. So you compared them. If you are doing only set theory, then you say maps to compare the sets.

(Refer Slide Time: 17:12)



So one more example of natural ring, I want to construct. These are so called polynomial rings. So first of all, I want to spend couple of minutes for polynomials. So polynomial means what? Polynomial means an expression like $a_0 + a_1 X + \ldots + a_n X^n$, $a_0, a_1, \ldots, a_n \in R$. So these are polynomials with coefficients in the ring R. It is an expression like this.

Now one may say what does one mean by expression? So one easy way to think about them is, you see, if you know the coefficients, you know the polynomial, but you should know the coefficients and their positions. So which coefficient goes where? So one way to think about them instead of this expression, think about a tuple, $(a_{0,} a_{1,} \ldots a_n, \ldots)$. It is not a finite tuple. It is a tuple, actually one should say $\mathbb{N}$ tuple.

That means the components in this tuple are numbered by using the set of natural numbers: 0, 1, 2, etcetera, n. So this tuple, I should have written here 0, after that 0, 0, 0, 0, all the way. So this tuple has entries, these are the components. So this tuple is an element of R, their entries are in R and their N tuple is denoted by like this, $R^{\mathbb{N}}$. So that is just a map from $\mathbb{N}$ to R. But we

have more than arbitrary map. We have only the finitely many coordinates of this tuple are non-zero. That I want to write in a notation like this: $R^{(\mathbb{N})}$.

This means they are n tuples with entries in R and only finitely many entries are non-zero. So eventually after some stage all the entries will become zero. So either think like this or think like expression like this. So this position a_1 you put a symbol X. This position you keep increasing the powers of X. So that is typically one thinks about polynomial. Also I want to remind you that when I said yesterday that the quadratic equations, cubic equations, bi-quadratic equations, et cetera, from there to progress to the arbitrary polynomials, it took longer time because there was no notation for polynomial.

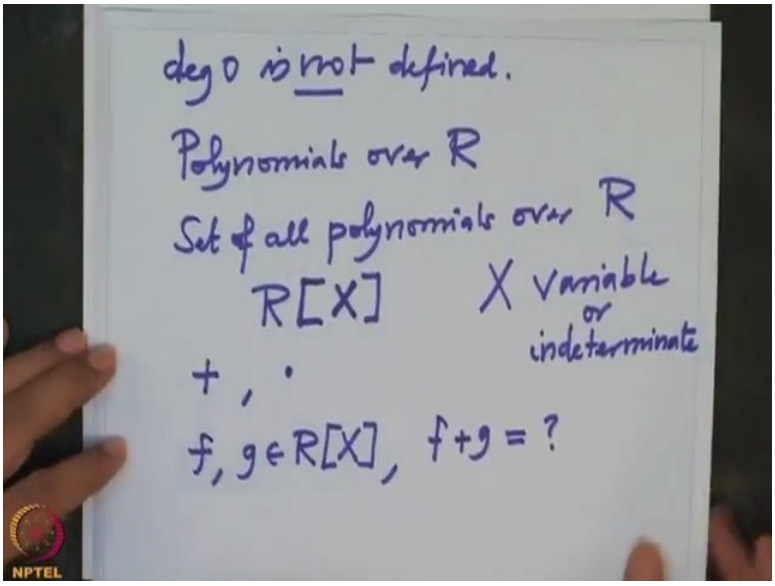
People at that time were not very careful in notations and also meanings and so on. So the person who did this first systematically was Viete. This was in 1591, he was a French mathematician. More about this I will say when I prove some result. So now if you have two polynomials, so polynomials are usually denoted by f(X). When there is no confusion, we will only write it f. f is a polynomial, that means expression like this.

Or if you want to think, think like coordinates. But I would recommend we start with this because we were used to that even from earlier curriculum like school, college, et cetera. So that is a polynomial. Where the last coefficient is non-zero, of course we only have to note up to where, where it is non-zero and after that there are zeroes. Now a_n, the last time when it is zero, that n is called the degree of this polynomial.

So this n is called the degree of f, if a a_n is non-zero. And all other terms are zero after that. a m is zero for all m bigger than n. Then this is called a degree. Let me remind you degree of, what is, 0 is also polynomial. These all the coefficients are 0, it is (0, 0, 0,...) tuple. So that is called a zero polynomial. So zero polynomial is same thing as 0. I will write it 0 because all coefficients are 0. But this is also the tuple (0,0,...).

And the degree is not defined then because what was the definition, there is only the last one which is non-zero. But there is no non-zero entry in this. So this degree of zero polynomial is not defined, that one should note carefully.

(Refer Slide Time: 22:58)

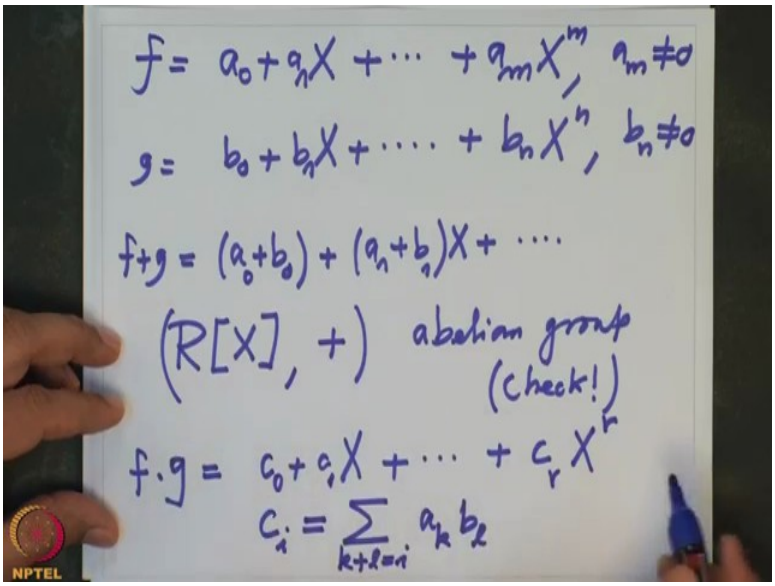


So degree of 0 is not defined. So also called polynomials over R. And the set of all polynomials over R is denoted by, set of all polynomials over R, this set is usually is denoted by R[X]. And remember my writing always variable. This X is called also variable. X is a variable or indeterminate. Variables and indeterminates are always denoted by X, because x are used, you will see, they will be used for evaluations.

So and this square bracket is also denoted for the polynomials. Later on I will say they are rational functions. So now on this set, there are two natural operations, addition and also multiplication, so that it becomes a ring and then we will say that it is a polynomial ring over a ring R. And what are these operations? So that means what? I have to write, if I have two polynomials f and g in R[X], then I have to tell you what is f plus g. This is what?

So very simple. You take f and g and think of them as tuples. So there are two tuples with, they are numbered by the natural numbers and only finitely many are non-zero. So I will add corresponding coordinates and put them as coefficients. Or think of this new tuple. So that is called the f + g. So let me write it only once.

(Refer Slide Time: 25:38)

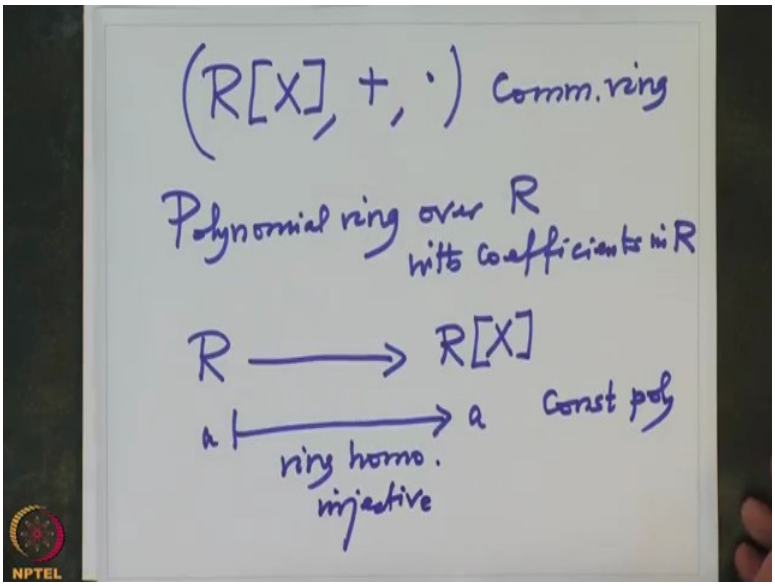


So if I have $f = a_0 + a_1 X + \ldots a_m X^m$; this a m is non-zero. So m is a degree of f. $g = b_0 + b_1 X + \ldots + b_n X^n$, where b_n is non-zero. And how do I add f plus+ g? That is you add the corresponding coordinates. $(a_0 + b_0) + (a_1 + b1)X + \ldots$ and so on. Now this may be bigger, that may be bigger, so add corresponding coefficients.

So you will, if they are equal, then you will interpret the same position, otherwise you will go on to the next one. So that is the addition of polynomials. Now one has to check that this addition is associative and the polynomial zero is the additive identity and with respect to plus+ these polynomials form an Abelian group. So this is Abelian group. This I will not check. I will simply say check. One has to check.

Similarly there is a product notation, that is given f and g like this. I want to define what is define what is f . g, or f multiplied by g. This is little complicated. So it is again, so f is like this, g is like this. When I want to write f time g, so I will write in this notation: $c_0 + c_1 X + \ldots c_r X^r$. Now I have to tell you, what are c in terms of a and b. So c_i is by definition $\sum_{k=1}^{i} a_k b_l$. Now remember this multiplication is in R and the sum is also in R.

(Refer Slide Time: 28:17)



So this definition makes it a multiplication on this set and with respect to that, now I will simply directly say that this (R[X],+,.), this is also commutative ring. And this ring is called a polynomial ring over R. Or also one says polynomial ring with coefficients in R. So we have extended the definition of addition and multiplication from the ring R to the polynomial. And we have the natural from R to R[X], namely a going to a. These are called the constant polynomials. And this is a ring homomorphism. Not only arbitrary homomorphism but this ring homomorphism is injective. That means it is injective as a map. That means different elements go to different images. Okay, we will continue our lecture after the break. Thank you.